***** PUBLIC VERSION *****

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

UNITED STATES OF AMERICA, Plaintiff, v. ZACKARY ELLIS SANDERS, Defendant.	Case No. 1:20-cr-00143 Honorable T.S. Ellis, III Trial: October 19, 2021 **HEARING REQUESTED**

MEMORANDUM IN SUPPORT OF RENEWED MOTION TO SUPPRESS BASED ON WARRANTLESS USE OF A NETWORK INVESTIGATIVE TECHNIQUE AND FALSE MATERIAL INFORMATION IN AFFIDAVIT PARAGRAPH 25

Zackary Ellis Sanders, by and through counsel, respectfully supplements the record and renews his motion to suppress all evidence obtained during the search of his family's home.[1] This motion is based on substantial evidence now available regarding the United States' integral role in the purportedly "independent" foreign law enforcement investigation that led to the search warrant in this case. As a result of the joint nature of that investigation, there are two related but independent grounds requiring suppression here: (1) that a Network Investigative

[1] This motion renews and supplements Mr. Sanders Motion to Suppress Based on False and Misleading Material Information in Affidavit Paragraph 25 (Motion to Suppress No. 4) (Dkt. 90-91). Mr. Sanders also incorporates by reference the following prior pleadings and related exhibits: Dkt. 109, 112, 137, 138, 140, 176, 241, 252, 253, 255, 256, 335, 354, 427, and 467.

Technique, CIPAV, or other form of code (collectively referred to as an "NIT")[2] was deployed to an Internet user's computer without a US warrant as part of the joint operation, in violation of Mr. Sanders's Fourth Amendment rights; and (2) that the FBI knowingly misled the Magistrate regarding the nature of this operation in seeking its warrant. This motion incorporates new evidence uncovered after the filing of Mr. Sanders's motions to suppress, such that the Court should consider the issues on a more complete record, "correct a clear error of law," and "prevent manifest injustice." *Zinkand v. Brown*, 478 F.3d 634, 637 (4th Cir. 2007).

In contrast to the approach other courts have taken, this Court declined to order further discovery regarding the government's knowledge of, and participation in, the law enforcement operation that led to the search of the Sanders family's home.[3] Mr. Sanders has accordingly been forced to rely entirely upon his own investigation of publicly available material. Nonetheless, based on that investigation, it is now more apparent than ever that the operation that resulted in the search warrant for the Sanders's home was a joint venture that included various US law enforcement agencies and the [redacted] ("[redacted] ("[redacted] It is

[2] "Privacy advocates refer to this type of process/technique as Malware. Other countries may have different names for [it]." Miller Decl. 1 (Dkt. 256-4) at ¶ 18. *See also infra* at n. 11. We use the term NIT or "active attack" to refer to a technique where (1) "malware . . . executes on the user's computer and forces it to directly connect to the Internet (as opposed to connecting through Tor)," or (2) a method "force[s] the user's Tor Browser to malfunction and connect directly through the Internet rather than sending network traffic through [Tor]." Murdoch Decl. (Dkt. 464-2) at ¶¶ 29-30. Under either scenario, such a technique "interferes with the user's computer." *Id.* at ¶¶ 29-30.

[3] *See, e.g., United States v. Mitrovich*, 458 F. Supp. 3d 961 (N.D. Ill. 2020) (ordering the government to disclose information about its ability to identify IP addresses and communications between the FBI and foreign law enforcement agencies); *United States v. Budziak*, 697 F.3d 1105, 1112-13 (9th Cir. 2012) (holding that it was "an abuse of discretion for the district court to deny . . . discovery on [a software program developed by the FBI that allowed it to see what files particular users were downloading]," reasoning that "criminal defendants should not have to rely solely on the government's word that further discovery is unnecessary . . . ").

further clear that, as part of that joint venture, the [redacted] utilized a method to identify IP addresses of computers in the US that interfered with, *inter alia*, Mr. Sanders's computer, by causing it to connect outside of Tor and transmit his IP address without his knowledge or authority. This was a warrantless search conducted in violation of the Fourth Amendment. *United States v. Darby*, 190 F. Supp. 3d 520, 530 (E.D. Va. 2016), *aff'd*, 721 F. App'x 304 (4th Cir. 2018) (deployment of an NIT that obtains information from a person's computer is a search and seizure). If, in the alternative, the [redacted] did not use an NIT, then it utilized a method—passive traffic analysis—that is insufficiently reliable to form the basis for a search warrant under these circumstances.

Because the legality of the identification and its reliability were necessary to the Magistrate's finding probable cause, the search warrant issued in this case was invalid and all evidence must be suppressed. Furthermore, because the Special Agent's misleading statements regarding the joint operation were made knowingly, or with reckless disregard for the truth, the good faith exception does not apply. *United States v. Leon*, 468 U.S. 897, 932 (1984).

FACTUAL BACKGROUND

A. US and [redacted] law enforcement jointly investigate online child pornography offenses.

The US has a longstanding practice of working hand-in-hand with foreign law enforcement agencies such as the [redacted] [redacted] in jointly investigating cybercrime, especially websites suspected of containing child pornography. *See, e.g.,* US Attorney's Bulletin (Dkt. 140-4) at 5 (stating that "[t]he global nature of online-facilitated crime . . . means that law enforcement *must frequently collaborate with international partners* to determine where criminal activity is occurring, as well as how evidence and criminal infrastructure can be seized.") (emphasis added); *id.* at 6-8 (highlighting Operation Pacifier as one example, where the FBI took over a website called Playpen, which contained child pornography, and deployed an NIT to

identify visitors and users of the website); [redacted] (emphasis added); Gov't Opp'n (Dkt. 43) at 16 (referring to the [redacted] as "a *familiar and reliable foreign counterpart* to the FBI") (emphasis added).

The FBI and the Department of Justice ("DOJ") have repeatedly recognized the [redacted] generally, and the [redacted] specifically, as its working partner. [redacted]

[redacted]

1. US law enforcement worked jointly with the [redacted] and other foreign law enforcement to investigate an onion service called [redacted]

Since sometime before 2017, Canadian and US law enforcement worked together to identify and arrest one of the administrators of an onion service website[4] called [redacted] *See, e.g.,* [redacted] News Story 1, attached as Ex. 3, at 2-3 [redacted] News Story 2, attached as Ex. 4, at 1-2 [redacted] News Story 3, attached as Ex. 5, at 3 (similar). After the [redacted] administrator pled guilty in late [redacted], the FBI and its foreign law enforcement partners continued to investigate the website.[5] On January 16, 2019, an FBI agent took various screenshots of [redacted] *See, e.g.,* Homepage (Dkt. 176-1) (indicating that the screenshot was captured on January 16, 2019).

[4] Onion services are websites that are only accessible via Tor. Miller Decl. 1 (Dkt. 256-4) at ¶ 7. They were previously called "hidden services," but the Tor Project, the non-profit that created the Tor Browser, now refers to them as onion services. Law enforcement still refer to them as "hidden services" or "dark web" sites. *Id.* at ¶ 7; Aff. (Dkt. 254-3) at ¶ 5(i).

[5] The government has itself described the large "scope of the government's investigation" as "obvious." Gov't Opp'n (Dkt. 244) at 11.

The [redacted] joined the FBI in investigating [redacted] along with many other onion service websites, as part of an operation the [redacted] called "[redacted] (and "[redacted] Inspection Report (Dkt. 138-1) at 11; Intel Log (Dkt. 254-1) (subject of report is "[redacted] *see also* FLA Report (Dkt. 253-3) (report from [redacted] "[d]isseminated to: International partners in receipt of [redacted] intelligence").[6] In the Affidavit in support of the Criminal Complaint in this case, FBI Agent Obie averred that "[t]he FBI, *in conjunction with other law enforcement entities*, is investigating websites on which visitors can access and view child sexual abuse material," including but not limited to [redacted] Obie Affidavit (Dkt. 4) at ¶ 9 (emphasis added); Gov't Opp'n (Dkt. 244) at 11 (same).[7]

The [redacted] claimed to have identified a large number of IP addresses of visitors to various onion service websites, including [redacted] that purportedly took place in April and May 2019. *See, e.g., United States v. Bateman*, No. 1:20-CR-10012-IT, 2021 WL 3055014, at *1 (D. Mass. July 20, 2021) at 1-2 (referencing visit to website on April 20, 2019); *United States v. David Corwin*, Case No. 2:21-cr-00218 (E.D.N.Y., March 23, 2021) (ECF No. 1, Complaint) ("*Corwin* Complaint") (Dkt. 354-9) at ¶ 3 (describing visit to website on April 27, 2019); FD-1057 (Dkt. 427, Ex. 5-B) at 2 describing visit to website on May 23, 2019); FLA Letter (Dkt. 253-2) (noting that the [redacted] had provided the FBI "*Internet addresses (IPs)*.") (emphasis added); Nov. 21, 2019

[6] Notwithstanding multiple defense motions to compel, the government has not disclosed the operation name the FBI used as its counterpart to "[redacted] and "[redacted] or the differences between those operations.

[7] The US and [redacted] agreed how they would use the information disseminated through this operation: "the FLA requested as a condition for providing its tip to the FBI that its identity, the existence of its investigation, and the information it provided not be publicly disclosed to the greatest extent possible." Gov't Opp'n (Dkt. 294) at 2.

Subpoena (Dkt. 335-2) (FBI administrative subpoena issued to Cox for records pertaining to 391 different IP address provided by the [redacted] including 98.169.118.39, on various dates).

According to the Affidavit, in June 2019, a foreign law enforcement agency "seized" the "computer server hosting" [redacted] which was not located in the US. Aff. (Dkt. 254-3) at ¶ 15.

2. *The [redacted] was jointly investigating target websites, with its international partners.*

According to a [redacted] government report, [redacted] (Dkt. 138-1) at 11; *see also* [redacted] (Dkt. 138-4) at 11. The [redacted] claims that by "[w]orking with partners," [redacted] has identified "a significant number of unique global [IP] addresses on [Tor]," most of which were not in the [redacted] (Dkt. 138-1) at 11.[8]

3. *As part of [redacted] the [redacted] shared IP address information with the US that resulted in the search of the Sanders family's home.*

[redacted] has operated by collecting and analyzing data from the [redacted] and its law enforcement partners to identify visitors to various onion service websites, and disseminating that information among partners. *See, e.g., id.* at 11; [redacted] (Dkt. 253-12) ([redacted] (emphases added).

[8] In other cases, the government has prosecuted individuals who, unlike this Internet user, registered an account, logged in, and then posted on [redacted] *See, e.g.,* [redacted] attached as Ex. 6, at ¶¶ 1, 6, 7.

Under [redacted] the [redacted] shared intelligence reports and other information with US law enforcement. On August 19, 2019, the [redacted] sent the FBI a number of intelligence reports, including one that identified the Sanders family's IP address and referenced "[redacted] [redacted] (Dkt. 254-1). The same day, the [redacted] sent US law enforcement numerous other intelligence reports for other IP addresses, with the same tip language.

On Sept. 16, 2019, six days after the FBI and Homeland Security Investigations ("HSI") issued administrative subpoenas to various Internet Service Providers ("ISPs") for records related to the IP addresses that the [redacted] provided, the [redacted] addressed a one-page letter to SSA [redacted] with the FBI's Child Exploitation Operational Unit. [redacted] Letter (Dkt. 253-2).[9] The letter purported to provide SSA [redacted] with justification for the FBI (and HSI) to seek additional information about the IP addresses for which SSA [redacted] had already issued at least one administrative subpoena. Sept. 10, 2019 Subpoena (Dkt. 335-1): *see also* Nov. 21, 2019 Subpoena (Dkt. 335-2) (administrative subpoena to Cox Communications, also issued by SSA [redacted] for records pertaining to 391 different IP addresses).[10] The [redacted] letter to SSA

[9] [redacted]. See *Bateman*, No. 1:20-CR-10012-IT at *1. In that case, HSI (which had been investigating [redacted] since at least 2017), issued an administrative subpoena to Comcast on Sept. 10, 2019 (the same date the FBI issued an administrative subpoena in this case), to identify which of its customers had visited [redacted] using IP address 73.142.30.140 on April 20, 2019. *Id.* at 1, 2. The HSI agent in *Bateman* stated that he was "an active member of a *multi-national, multi-agency working group that coordinates* national and *international operations to combat child exploitation on the dark web*." *Bateman* Criminal Complaint, attached as Ex. 7, at ¶ 1 (emphases added).

[10] Both the Sept. 10, 2019 and Nov. 21, 2019 administrative subpoenas were issued by FBI SSA [redacted] as part of a larger investigation run by FBI headquarters ([redacted]). *See e.g.,* Ferrante Decl. (Dkt. 274-5) at ¶ 12; Nov. 21, 2019 Subpoena (Dkt. 335-2) (referencing [redacted]). The government has explained that the September subpoena was part of this same case and was later re-serialized. *See, e.g.,* FD-1057 (Dkt. 427, Ex. 5-B) at 2 (referencing [redacted]).

[redacted] stated that the [redacted] "ha[d] provided data to the [FBI] in relation to Internet addresses (IPs),"and that such IP data had been "lawfully obtained under the [redacted]" under "[redacted][11] "warrants." *Id.* The [redacted] also stated that this had been an "independent investigation" and that "at no time was any computer or device interfered with in the [US]." *Id.*

In February 2020, Agent Ford submitted his Affidavit. Agent Ford stated that (1) the [redacted] had obtained information about the IP address's purported activity "through independent investigation;" (2) that US law enforcement "did not participate in the investigative work through which the [redacted] identified the IP address information" and (3) that the [redacted] "had not interfered with, accessed, searched, or seized any data from any computer in the United States in order to obtain that IP address information." Aff. (Dkt. 254-3) at ¶ 25.

B. There were only two possible methods the [redacted] could have used to identify the Sanders family's IP address.

There were only two possible methods the [redacted] could have used to identify the Sanders family's IP address as having accessed an onion service website. *See, e.g.,* Murdoch Decl. (Dkt. 464-2) at ¶ 41 ("the Tor Browser disables technologies that could disclose identifying information"); *id.* at ¶ 44 ("[w]hen visiting a Tor Onion Service, an exit node is not used because data never leaves [Tor]").

To begin with, it is necessary to understand some features of the Tor, onion service websites, and [redacted] law, which helps explain how visitors to an onion service must have been identified. These explanations are based on the opinions of experts with backgrounds in Tor,

---

[11] "[redacted] stands for "[redacted] Decl. 1 (Dkt. 254-7) at ¶ 6; *see also* [redacted] Decl. 2 (Dkt. 254-8) at ¶ 3. [redacted]

computer science, law enforcement techniques that have been used to identify Internet users, and [redacted] police surveillance and investigatory powers. Dr. Richard Clayton is the Director of the Cambridge Cybercrime Centre at the University of Cambridge, and his "long-standing research interest [is] in how it is possible to trace people who are communicating over the Internet and when this may fail." Clayton Decl. (Dkt. 256-8) at ¶ 1. Dr. Steven Murdoch is the Professor of Security Engineering at University College London who obtained his Ph.D. from the University of Cambridge Department of Computer Science and Technology. Murdoch Decl. (Dkt. 464-2) at ¶ 1. He has worked with Tor developers since 2004, created the first version of the Tor Browser software in 2008, and continues to work with the Tor Project to improve Tor's security and usability. *Id.* at ¶ 2. Dr. Matthew Miller worked as an Associate Professor of Computer Science and Information Technology at the University of Nebraska at Kearney. Miller Decl. 1 (Dkt. 256-4) ¶ 1. Seth Schoen is a computer technologist and privacy specialist who worked as a Senior Staff Technologist for 19 years at the Electronic Frontier Foundation, a non-profit that specializes in Internet privacy, during which time Mr. Schoen assisted in Tor's development and worked with Tor developers. Schoen Decl. (Dkt. 256-7) at 1, 15-16. [redacted] who has been practicing in the [redacted] for 27 years and a part-time judge in the higher criminal courts, with an expertise in law enforcement powers.

1. The Tor network and the Tor Browser

The Tor Browser is a software program that allows Internet users to connect to the Internet through the Tor network to browse both the open Internet and onion services, while benefiting from heightened security protections. Miller Decl. 1 (Dkt. 256-4) at ¶ 7; Miller Decl. 4 (Dkt. 256-6) at ¶¶ 9-10; Schoen Decl. (Dkt. 256-7) at ¶¶ 7-12, 21, 31; Clayton Decl. (Dkt. 256-8) at ¶¶ 36-37. The Tor Browser is a web browser like Microsoft Edge, Google Chrome and

Mozilla Firefox, that connects to the Internet through the Tor network and provides additional privacy protections to preserve users' anonymity, including not revealing their IP addresses. Miller Decl. 4 (Dkt. 256-6) at ¶¶ 11-12; Schoen Decl. (Dkt. 256-7) at ¶¶ 31-38, 42.

Together, the Tor network and the Tor Browser protect users' privacy by passing encrypted data packets (also known as traffic) through a random circuit of at least three of the thousands of Tor nodes around the world. Miller Decl. 1 (Dkt. 256-4) at ¶¶ 12-15; Miller Decl. 4 (Dkt. 256-6) at ¶¶ 4-8; Clayton Decl. (Dkt. 256-8) at ¶¶ 20-30.[12] As traffic travels from an Internet user's computer to a website, a circuit is built up using these nodes; because the nodes are randomly selected and are independent from one another, it is "impossible for any [of these nodes] to know both the original source and the final destination of the [traffic] being passed." Clayton Decl. (Dkt. 256-8) at ¶ 28. Furthermore, "[t]here is also some data padding going on so that the amount of data . . . will not act as a distinguishing feature to allow circuits to be traced." *Id.* at ¶ 27. Thus, when a user visits a particular website using Tor, "[i]nstead of the user's own IP address, [a] website operator would see the connection appear to originate from a so-called Tor exit node." Schoen Decl. (Dkt. 256-7) at ¶ 30.

2. Onion service websites

Onion services are websites that are accessible only through the Tor network, and which have six nodes between them and a Tor user in order to protect both the anonymity of the onion service's IP address and the anonymity of the Internet user's IP address. *See* Murdoch Decl. (Dkt. 464-2) at ¶¶ 6, 8-10; *see also* Clayton Decl. (Dkt. 256-8) at ¶¶ 31-35 (similar). When an

[12] *See also Tor: Overview*, The Tor Project, available from https://2019.www.torproject.org/about/overview.html.en (last accessed Sept. 24, 2021) (an overview of what Tor is and how it works from the Tor Project, the 501(c)(3) non-profit, supported by the US government, that created the Tor Browser).

onion service website and an Internet user's computer "exchange information, i.e., the user's web browser . . . request[s] to view a web page" and "the Onion Service . . . respond[s] with the requested content," the user and the website are connected by "the guard node selected by the user's computer, one middle node, the rendezvous node, two middle nodes, and the guard node selected by the Onion Service." Murdoch Decl. (Dkt. 464-2) at ¶¶ 10-11. The six-node "design means that, without collaboration between all of the nodes on one of the Tor circuits, no entity can ever learn who anyone else is [or] where the [Onion] service is located:" for example, "[e]ven if the user (or indeed the [onion] service) deliberately chooses compromised nodes . . . since the second half of the message transfer takes place over a circuit chosen by the other party, there is no information leakage." *Id.* at ¶ 35. When a Tor user visits an onion service website, "an exit node is not used because data never leaves the Tor network." *Id.* at ¶ 44.

3. Either an NIT—which interferes with a user's computer—or passive traffic analysis—which is error prone—was used in this case.

Because of the unique security features of Tor, law enforcement cannot use the same techniques they would traditionally use to identify IP addresses on the open Internet. Aff. (Dkt. 254-3) at ¶ 8 ("Because of the way the Tor network routes communications through the relay computers, traditional IP-address-based identification techniques are not effective."); Operation Torpedo NIT Warrant (Dkt. 354-4) at ¶ 7 (similar).

Law enforcement can attempt to de-anonymize the IP address of an Internet user visiting an onion service website in either of two ways: (1) an active attack (such as an NIT) that interferes with a user's computer, or (2) passive traffic analysis, which is statistical in nature and error prone. Clayton Decl. (Dkt. 256-8) at ¶¶ 42-52; *see also* Murdoch Decl. (Dkt. 464-2) at ¶¶ 23-31. Here, where there is no allegation that the Internet user disclosed identifying information, there is no other method. *Id.* at ¶ 23.

"In an active approach, law enforcement uses their physical access to the server to arrange for it to send content which will serve to identify the user." Clayton Decl. (Dkt. 256-8) at ¶ 42. Such an active attack is commonly referred to as an NIT. To use an NIT, "law-enforcement *must* control the Onion Service prior to deploying the NIT." Murdoch Decl. (Dkt. 464-2) at ¶ 28 (emphasis added). Once law enforcement controls an onion service website, it can "place[] content onto [the onion service website] which," because of some type of malware or exploit "makes the user's machine access an Internet resource over the open Internet rather than over a TOR circuit" and reveal the user's IP address. Clayton Decl. (Dkt. 256-8) at ¶ 46. However, "[t]he TOR browser has been specially developed to prevent this type of information leakage, so it is only by adding special content," such as malware or using an exploit, "that law enforcement can identify the user." *Id.* at ¶ 46.

In a passive approach, "traffic to and from the hidden service is compared with traffic between the user's machine and a TOR node," without being able to trace the entire path traffic takes. Clayton Decl. (Dkt. 256-8) at ¶ 47. It is a technique that attempts "to identify which user is communicating with which Onion Service by comparing patterns of when and how much data is sent (as opposed to looking at the content of the data, which is not visible to observers)." Murdoch Decl. (Dkt. 464-2) at ¶ 17. "[T]he problem with [traffic analysis] is that the identification being made is statistical in nature – this traffic looks like that traffic (in terms of size), and is similar in timing, but delayed a bit . . . . However, it might look like some other traffic as well and hence it would be wrong for law enforcement to conclude they had the right IP address if there was only one measurement event – so a single visit to a[n onion service website] could be misidentified." Clayton Decl. (Dkt. 256-8) at ¶ 50. Furthermore, prior to May 2019, the Tor Project implemented a number of measures "to make it even more difficult to use traffic-

analysis to de-anonymize Tor users." Murdoch Decl. (Dkt. 464-2) at ¶ 21; *see also id.* at ¶¶ 15-20 (explaining, *inter alia*, how the growth of the Tor network, Tor's requirement that it take 68 days for a new node to run at full capacity and thereby prevent anyone from quickly creating new nodes in an attempt to monitor traffic passing through them, the random addition of padding data to and from guard nodes to hide patterns in data rates,[13] and the Tor Project's actions to pro-actively identify and exclude questionable nodes are measures put in place, prior to May 2019, to make traffic analysis not viable as a reliable method of identifying IP addresses in May 2019).

4. Although the government has never explained how the Sanders family's IP address was identified, the methods described by Agent Ford in his August 2020 declaration would have not been viable in May 2019.

Apart from Agent Ford's declaration (Dkt. 254-12), the government has never explained how the [redacted] identified the Internet user's IP address. In August 2020, after Mr. Sanders argued in a motion to compel that the [redacted] had likely interfered with his computer, Agent Ford submitted a declaration stating that he had since "learned," "researched," and "discussed . . . with others" the "ways for Tor users to be de-anonymized and identified through their use of the Tor network that do not involve interference with the users' computer devices, consistent with the information provided by the [redacted] *Id.* at ¶¶ 3-4. None of the methods Agent Ford referenced are applicable to this case. *See, e.g.,* Murdoch Decl. (Dkt. 464-2) at ¶¶ 33-44 (explaining why Agent Ford's declaration cannot explain what how the [redacted] identified the Sanders's IP address and misstates what is possible with a user visiting an onion service website).

First, Agent Ford cited 2004 and 2008 research papers that discussed the "global passive adversary." Ford Decl. (Dkt. 254-12) at ¶ 7. The global passive adversary is a "theoretical

[13] [redacted] "GCHQ noted a high level of errors in performing traffic-analysis on Tor, even before the extended padding feature was introduced in 2016." Murdoch Decl. (Dkt. 464-2) at ¶ 19.

process" that "[a]cademics, researchers, and computer scientists have discussed . . . but have not seen . . . used in practice." Miller Decl. 3 (Dkt. 254-5) at ¶ 5. "Neither [of the papers] show that the global passive adversary is possible" instead, it is a "theoretical assumption," in other words, "a helpful thought experiment for research," that "does not . . . imply that such an adversary could ever exist in the real world." Murdoch Decl. (Dkt. 464-2) at ¶¶ 34-37. Since those papers were published, "[t]he Tor Browser and the Tor network have been adapted many times to prevent the types of attacks that the Special Agent describes theoretically." Miller Decl. 3 (Dkt. 254-5) at ¶ 6. "[E]ven the most capable intelligence agencies such as NSA or GCHQ cannot achieve th[e] goal [of being a global passive adversary]." Murdoch Decl. (Dkt. 464-2) at ¶ 36; *see also* Clayton Decl. (Dkt. 256-8) at ¶¶ 56-58.[14]

Second, Agent Ford cited a paper that described an unreliable confirmatory method of traffic analysis that was only possible when law enforcement controlled the onion service, was on the same continent as the user, and was able to manipulate traffic only to attempt to confirm an identification when law enforcement already knew the IP address of the user. This so-called confirmatory method has been made much more difficult since 2008, *see supra* at 13-14, and "is

[14] A 2012 US report distributed by the National Security Agency ("NSA") to its Five Eyes partners, [redacted], noted the following: "[w]e will never be able to de-anonymize all Tor users all the time. With manual analysis we can de-anonymize a **very small fraction** of Tor users, however **no** success de-anonymizing a user in response to a TOPI request/on demand." Tor Stinks, Presentation by NSA, published by The Guardian (Oct. 4, 2013), available from https://edwardsnowden.com/2013/10/04/tor-stinks-presentation/ (last accessed Sept. 14, 2021), attached as Ex. 8, at 2 (emphases in original); *see also id.* at 23 ("We can increase our success rate," but "[w]ill never get 100% but we don't need to provide true IPs for every target every time they use Tor."). However, "[s]ince then, the [Tor] network capacity has grown from about 10 gigabits per second to 200 gigabits per second," which has increased the difficulty of performing the manual analysis discussed by the NSA "by a factor of 20." Murdoch Decl. (Dkt. 464-2) at ¶ 15.

not relevant to understanding what law enforcement could have done in 2019." Murdoch Decl. (Dkt. 464-2) at ¶ 38.

5. [redacted]

The information about what a [redacted] warrant authorizes is publicly available. [redacted] Decl. 1 (Dkt. 254-7) at 2. Thus, "it would be self-evident to any person working with data gathered under a [redacted] warrant, that it is almost meaningless unless the context in which it was gathered is clear. . . . Where the risk of 'collateral intrusion' and the gathering of data relating to those with no criminal purpose is significant[,] such data has little, if any, probative or evidential value." [redacted] Decl. 1 (Dkt. 254-7) at ¶¶ 12-15.

6. The FLA clearly used an active attack to interfere with users' computers in the US in order to identify their IP addresses.

It is obvious that the FLA used an active attack in this case to cause users' computers to reveal their IP addresses. Clayton Decl. (Dkt. 256-8) at ¶¶ 60-63; Miller Decl. 1 (Dkt. 256-4) at

¶¶ 17-19; Murdoch Decl. (Dkt. 464-2) at ¶¶ 22-32. Such a technique "necessarily interferes with a user's computer wherever it is located." *Id.* ¶ 32. The government has the burden of showing that the FLA did not use such an attack. *See* e.g., *Fla. v. Harris*, 568 U.S. 237, 248 (2013) ("If the State has produced proof from controlled settings that a dog performs reliably in detecting drugs, and the defendant has not contested that showing, then the court should find probable cause. If, in contrast, the defendant has challenged the State's case (by disputing the reliability of the dog overall or of a particular alert), then the court should weigh the competing evidence.").

The FLA was unlikely to use traffic analysis, as it is "extremely unlikely to yield the hundreds of IP addresses submitted by the [FLA], nor give the [FLA] confidence that these IP addresses visited the Onion Service in question." Murdoch Decl. (Dkt. 464-2) at ¶ 31. And an identification of an IP address using traffic analysis that is based only on a single visit "could very well be a false-positive error." *Id.* at ¶ 32; *see also* Clayton Decl. (Dkt. 256-8) at ¶ 59 (similar). Furthermore, "[i]improvements in the Tor network's design and operation prior to May 2019 have made traffic analysis [even] less reliable and more difficult to execute." Murdoch Decl. (Dkt. 464-2) at 3.

In the past, for the reasons discussed above, the FBI has "used a process that interfered with Tor Browser's security protections to take control of, access, interfere with and/or search the contents of computers that visited a particular website accessed through the Tor Network." Miller Decl. 1 (Dkt. 256-4) at ¶ 18; *see also* Miller Decl. 4 (Dkt. 256-6) at ¶¶ 16-17. *See, e.g.*, *United States v. Levin*, 186 F. Supp. 3d 26, 30–31 (D. Mass. 2016), *vacated and remanded*, 874 F.3d 316 (1st Cir. 2017) (describing use of NIT warrant and Title III warrant in Operation Torpedo); *United States v. Cottom*, 679 F. App'x 518, 519 (8th Cir. 2017) (describing use of NIT warrant in Operation Torpedo); Eric Marques (FreedomHosting)

Assistant Director Report, Complaint, and Statement of Facts (Dkt. 354-5) (demonstrating that the FBI took control of the FreedomHosting server after a tip from a foreign law enforcement agency, and that mutual legal assistance treaties and Title III warrant(s) were used); *United States v. Austin*, 230 F. Supp. 3d 828, 831 (M.D. Tenn. 2017) (describing use of NIT warrant and Title III warrant in Operation Pacifier (Playpen) cases); *United States v. Michaud*, No. 3:15-CR-05351-RJB, 2016 WL 337263, at *1–2 (W.D. Wash. Jan. 28, 2016) (similar).

C. Joint ventures between international partners are necessary for law enforcement to locate and take control of onion services and to then identify visitors to them.

In the past, once foreign law enforcement identified a particular site, US law enforcement would take control of the website, using various means. This took place in the FBI's major operations to shut down child pornography sites, including in Operation Torpedo, FreedomHosting, and Operation Pacifier. *See, e.g.,* Operation Torpedo NIT Warrant (Dkt. 354-4) at ¶ 9 (application for search warrant to deploy NIT against visitors to 'Bulletin Board A,' after being alerted to its location and contents by an FLA); *see also* Kevin Poulsen, *FBI Admits It Controlled Tor Servers Behind Mass Malware Attack*, Wired, (Sept. 13, 2013), https://www.wired.com/2013/09/freedom-hosting-fbi/ (last accessed Sept. 22, 2021) (explaining that the government malware used in the FreedomHosting operation was a code that exploited a vulnerability in the Tor Browser forcing computers to send identifying information through the open internet); *United States v. Knowles*, 207 F.Supp.3d 585, 592-93 (D. S.C. Sept. 9, 2016) (explaining that "[t]he NIT would 'augment' the normal content Playpen sends to users with 'additional computer instructions' that 'are designed to cause the user's 'activating' computer to transmit certain information to a computer controlled by or known to the government."). In all of those operations, the FBI worked with foreign law enforcement agencies and relied on domestic warrants to deploy NITs (and some combination of Title III warrants and/or pen-trap

and trace registers). Furthermore, SSA [redacted] the agent to whom the [redacted] addressed its Sept. 16, 2019 letter and is the agent listed on two administrative subpoenas disclosed in discovery—was involved in both Operation Torpedo and FreedomHosting. *See, e.g.,* [redacted].

While running the website, US law enforcement then deployed a technique to cause the computers of Internet users to connect to a website outside of the Tor network or send identifying information to a server, which would reveal their IP addresses. Without the deployment of such a technique, Internet users' computers would otherwise remain inside Tor, and would not reveal their IP addresses. US law enforcement has previously stated that such a technique is the only one they are aware of for de-anonymizing Tor users. Mot. to Suppress (Dkt. 254) at 10-11 (collecting examples).

ARGUMENT

I. THE EXCLUSIONARY RULE APPLIES TO THE [redacted] ACTIONS.

"Ordinarily, the fourth amendment does not apply to . . . searches made by foreign authorities in their own country and in enforcement of foreign law," however, two exceptions exist: first, "if American officials participated in the foreign search" or the foreign officials were "acting as agents for their American counterparts," and second, if "the conduct of the foreign officers shocks the conscience of the American court." *United States v. Heller*, 625 F.2d 594, 599 (5th Cir. 1980); *see also United States v. Abu Ali*, 528 F.3d 210, 228 (4th Cir. 2008) (quoting *Heller*). Here, the exclusionary rule should be invoked because both exceptions apply.

A. Because US and [redacted] law enforcement engaged in a joint venture, the exclusionary rule applies to conduct by the [redacted]

Under the joint-venture doctrine, "if U.S. agents substantially participate in an extraterritorial search of a U.S citizen and the foreign officials were essentially acting as agents for their American counterparts or the *search amounted to a joint operation* between American and foreign authorities, the Fourth Amendment generally applies." *United States v. Stokes*, 726 F.3d 880, 890-91 (7th Cir. 2013) (emphasis added); *see also Abu Ali*, 528 F.3d at 228; *United States v. Behety*, 32 F.3d 503, 510–11 (11th Cir.1994) (similar); *United States v. Peterson*, 812 F.2d 486, 490 (9th Cir.1987) (similar).[15]

Here, the collaboration between US and [redacted] law enforcement was so substantial that it must be considered a joint venture. US and Canadian law enforcement, *inter alia*, initially began investigating the website. Eventually, both the FBI and the [redacted] were monitoring the site at the same time in 2019. *Supra* at 5-7. This was no coincidence. Indeed, given the history of the relationship between the US and the [redacted] generally and the FBI and the [redacted] specifically, it is inconceivable that each country was acting in isolation:. The US and the [redacted] and the [redacted] and the FBI have often jointly led cybercrime investigations, frequently including child pornography websites. *Supra* at 3-5. As part of this operation, the [redacted] received data from international partners (including the FBI), analyzed data

[15] Here, if the [redacted] used an NIT, this should not be considered an extraterritorial search. In that instance, a computer located in the United States was interfered with and searched and seized within the meaning of the Fourth Amendment.

[16] [redacted]

from partners, and also disseminated data to such partners. [redacted] (Dkt. 253-12) (seeking individual to "deal[] with volume data acquisitions of CSE material received from operations and international law enforcement partner community" and referencing "[redacted] FLA Report (Dkt. 253-3).

Statements by the FBI, the government, and the [redacted] concerning their own investigation and operation show that the joint venture doctrine applies to the investigation of [redacted] and the identification of IP addresses that purportedly visited [redacted] In seeking the arrest warrant for Mr. Sanders, Special Agent Obie averred that this investigation was conducted "in conjunction" with other law enforcement entities. Obie Affidavit (Dkt. 4) at ¶ 9. The government describes the [redacted] as a "familiar and reliable foreign counterpart" to the FBI, Gov't Opp'n (Dkt. 43) at 16, and has repeatedly emphasized the importance of the "cooperative relationship" between the FBI and the [redacted] Gov't Opp'n (Dkt. 294) at 2, 8. Discovery from the [redacted] itself refers to intelligence having been disseminated only to the [redacted] "international partners," FLA Report (Dkt. 253-3), which the FBI only received after first assuring its foreign counterpart and long-time partner that it would keep such information non-public to the "greatest extent possible," Gov't Opp'n (Dkt. 294) at 2, 8.

What the FBI did here is similar to the joint operation in *Peterson*, 812 F.2d at 490, where the DEA passed along information so that Philippine authorities could set up surveillance that would benefit the DEA's own investigative purposes. In *Peterson*, the Ninth Circuit held that the District Court "erred in concluding that the operation was not a joint venture." *Id.* at 490. There, as here, the foreign law enforcement agency appears to have initiated its investigation after receiving information from the US about drug smuggling through its country, and information continued to be exchanged between the two partners. *Id*. at 488. The foreign

law enforcement agency subsequently initiated surveillance efforts: the Philippine authorities placed wiretaps on people suspected of being involved with the shipment. *Id.*at 488-89. The Philippines then provided the DEA with the intercepts. *Id.*

After the US began investigating [redacted] the [redacted] began identifying visitors to the website. According to [redacted] government reports, the [redacted] worked with its "international partners," which necessarily includes the US and the FBI, to identify the IP addresses of visitors to the site. [redacted] Inspection Report (Dkt. 138-1) at 11. This also entails a back and forth of information. *See, e.g.,* [redacted] (Dkt. 253-12); *compare also* Intel Log (Dkt. 253-1) *with* [redacted] Letter (Dkt. 253-2) *with* FLA Report (Dkt. 253-3) (comparison showing it is not plausible that these three, one-page documents were transmitted, unsolicited, once a month for three months to various US officials and without response or request from the US). The [redacted] and the FBI communicated about exchanging information prior to the [redacted] passing on "tips" about those IP addresses to the FBI. *See supra* at n. 7.

This Court should scrutinize the government's representations here and compare them to how the DOJ, FBI, and [redacted] have described their previous investigations. Indeed, in Operation Pacifier (the Playpen investigation), the FBI concealed the "scope of the international aspect of the investigation" from both courts and the defense. Internal FBI Email (Dkt. 138-9) at 1 (discussing information that the FBI "want[ed] to continue to protect," that had "not been disclosed in any filings" or to the defense, including the "scope of the international aspect of the [Playpen] investigation"). The fact that the [redacted] directed its Sept. 16, 2019 letter to SSA [redacted] is also significant: as SSA [redacted] previously stated in an earlier case, child exploitation investigations "*require*[] the cooperation between the FBI and other countries." FD-302, attached as Ex. 9, at 1. In that case, the Court declined to credit SSA [redacted]

representations that it was "not a joint operation." *Mitrovich*, 458 F. Supp. at 967. This Court should similarly decline to credit the FBI's self-serving representations here. Based on the FBI's and government's own statements, discovery, and material from the [redacted] uncovered by the defense, the US and [redacted] were both substantially involved in the [redacted] investigation, and when the [redacted] identified the Sanders family's IP address, the [redacted] was acting as an agent of US law enforcement. Accordingly, the exclusionary rule applies.

B. Because the conduct by US and [redacted] law enforcement shocks the conscience of an American court, the exclusionary rule applies.

It is "well-established" that the Fourth Amendment applies if "the conduct of the foreign police shocks the judicial conscience." *United States v. Valdivia*, 680 F.3d 33, 51 (1st Cir. 2012). Courts have "inherent supervisory powers over the administration of federal justice" and must apply the Fourth Amendment to evidence seized by foreign authorities when their conduct is so egregious. *United States v. Emmanuel*, 565 F.3d 1324, 1330 (11th Cir. 2009). Courts have long-criticized egregious law enforcement conduct, particularly when their actions affect third parties who are not investigation targets. *See United States v. Archer*, 486 F.2d 670, 672, 676-77 (2nd Cir. 1973) (holding that "[g]overnmental 'investigation' involving participation in activities that result in injury to the rights of its citizens is a course that courts should be extremely reluctant to sanction"); *see also United States v. Thoma*, 726 F.2d 1191, 1199 (7th Cir. 1984) ([W]e will closely examine [cases where] the Government misconduct injures third parties in some way.").

The [redacted] and FBI's conduct shocks the judicial conscience and requires application of the exclusionary rule for three reasons: (1) the [redacted] has worked with US authorities to conceal US involvement in this operation in order to evade the Fourth Amendment; (2) the [redacted] used a technique that interfered with computers in the US (or, if not, used a technique that was too

unreliable to identify the many IP addresses it did); and (3) the US and the [redacted] took actions to allow the distribution of child pornography to persist, under their watch.

First, the FLA provided the Sept. 16, 2019 letter in response to a request from the FBI, in order to justify the FBI's subpoenaing of various ISPs. *See supra at* 8-9. Second, [redacted] authorities using a technique that interferes with US computers, without a warrant, in a direct circumvention of the Fourth Amendment, is conduct that shocks the conscience of an American court. *United States v. Owens*, 2016 WL 7053195, at *5, n.1 (E.D. Wis. Dec. 5, 2016) ("Various district courts have already addressed the issue in relation to the specific NIT warrant in this case. The Court agrees with the majority of courts finding a Fourth Amendment search occurred."); *see infra* at 25-28. In the alternative, [redacted] authorities using a technique that cannot be relied upon to produce an accurate identification of an IP address and that yields an unknowable number of potential false positives as sufficient for establishing probable cause is conduct that shocks the judicial conscience. *See infra* at 28-29.

Third, if the government's descriptions of [redacted] are accurate, which the defense disputes, the US and [redacted] investigation of the website, which spanned several years, resulted in the continued distribution of child pornography, long past the point at which it appears US law enforcement partners could have shut down the site. *See supra* at 5-7. The Supreme Court has stated that anyone who distributes child pornography is culpable for the harm it inflicts upon children. *See Paroline v. United States*, 572 U.S. 434 (2009) ("The unlawful conduct of everyone who reproduces, distributes, or possesses the images of the victim's abuse . . . plays a part in sustaining and aggravating this tragedy."); *see also New York v. Ferber*, 458 U.S. 747, 759 (1982) (similar).

Federal courts have firmly criticized law enforcement misconduct while investigating child pornography offenses. *See e.g., United States v. Chin*, 934 F.2d 393, 395-96 (2nd Cir. 1991) (distinguishing the investigator's conduct from "the usual undercover operation" because it encouraged the defendant to "go out and commit a real crime" and raised "very serious concerns with respect to . . . the rights of the children Congress sought to protect."). The Playpen operation, during which law enforcement had only controlled the server for less than two weeks, was also heavily criticized by courts. *See United States v. Anzalone*, 221 F.Supp.3d 189, 194-95 (D. Mass. Sep. 28, 2016) (finding it "troubling that an agent stated the Producer's Pen [a section of the site] would be returning . . . because that section might have encouraged members to . . . share new child pornography"). Here, it appears that part of the purpose of the US and [redacted] operation was to continue to run the site in order to attract and identify new users. In this case, law enforcement likely controlled the server from at least April 2019, when Internet users were initially identified as having visited the site. Murdoch Decl. (Dkt. 464-2) at ¶¶ 22-32.

II. ALL FRUITS OF THE ILLEGAL IDENTIFICATION OF THE SANDERS FAMILY'S IP ADDRESS MUST BE SUPPRESSED BECAUSE IT WAS A SEARCH CONDUCTED WITHOUT A WARRANT.

Because it was a joint operation, the Fourth Amendment's prohibition against unreasonable searches and seizures required the FBI to obtain a valid, domestic warrant in this case before it allowed and worked with the [redacted] to de-anonymize the IP address of a computer in the United States browsing on the Tor network. A domestic warrant was required before intruding upon Mr. Sanders's computer because Internet users have a reasonable expectation of privacy in the contents of their computers and in their true IP address when they browse on the Tor network. *Darby*, 190 F. Supp. 3d at 530 (deployment of a NIT that obtains data from a person's computer is a search and seizure under the Fourth Amendment).

While something "a person knowingly exposes to the public" is not constitutionally protected, something a person "seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *Katz v. United States*, 389 U.S. 347, 351 (1967). For an "intrusion into [the] private sphere" to constitute a "search," an individual must "seek[ ] to preserve something as private," and society [must be] prepared to recognize [that expectation] as reasonable." *Carpenter v. United States*, 138 S. Ct. 2206, 2213 (2018) (quotation marks and citation omitted). The Supreme Court has already found that individuals have a reasonable expectation of privacy in their cell phone, due to the amount of personal information contained therein. *Riley v. California*, 134 S. Ct. 2473 (2014). The *Riley* Court also referred to cell phones as "minicomputers," implying that one has a greater expectation of privacy in a computer's contents than they would in their phone. *Id*. at 394; *see also United States v. Lifshitz*, 369 F.3d 173, 190 (2d Cir. 2004); *Trulock v. Freeh*, 275 F.3d 391, 403 (4th Cir. 2001); *Gust v. Leis*, 255 F.3d 325, 333 (6th Cir. 2001). Because "[a] personal computer is often a repository for private information the computer's owner does not intend to share with others. . . . it seems natural that computers should fall into the same category as . . . other personal items that command[ ] a high degree of privacy." *United States v. Andrus*, 483 F.3d 711, 718 (10th Cir.), *decision clarified on denial of reh'g*, 499 F.3d 1162 (10th Cir. 2007) (quotation marks and citation omitted). When an Internet user browses the open Internet using a non-Tor Browser, he voluntarily discloses information from his computer, his IP address, to those websites; however, that is not the case with the Tor Browser and with an onion service. *United States v. Taylor*, 935 F.3d 1279, 1282-83 (11th Cir. 2019) (explaining privacy differences between the open Internet and Tor). By using Tor, Internet users make efforts to keep their true IP addresses and the contents of their personal computers private. People also have the right to exclude others from their IP addresses.

See, e.g., Kaiser Aetna v. United States, 444 U.S. 164, 176 (1979) (calling the right to exclude "one of the most essential sticks" in the property rights bundle). Here, the Tor "node" is the bailee, and it owes a duty to the bailor, Mr. Sanders, to keep his data safe. *Carpenter*, 138 S. Ct. at 2268-69 (Gorsuch, J., dissenting) ("[e]ntrusting your stuff to others is bailment.").

People have a reasonable expectation of privacy in information contained on their computers, including their IP address, when using Tor because "only the IP address of the last relay computer . . . as opposed to the Tor user's actual IP address, appears on that website's IP address log," and furthermore, "the content of a Tor user's communications are encrypted." Aff. (Dkt. 254-3) at ¶ 11; *see also* Miller Decl. 4 (Dkt. 256-6) at ¶¶ 4-8; Clayton Decl. (Dkt.) at ¶¶ 20-35; Murdoch Decl. (Dkt. 464-2) at ¶¶ 8-11. The fact that a person seeks to preserve their Tor browsing as private means that it is constitutionally protected.

Here, because [redacted] was an onion service website, no Internet user voluntarily disclosed his IP address to [redacted] Unlike an Internet user on the open Internet, Tor users who are involuntarily redirected to the open Internet through the use of an NIT have their computers controlled by the government in an effort to search and seize information they are trying to keep private. *See Riley*, 134 S. Ct. at 2492-93 (finding a distinction between evidence about phone usage obtained from the phone company and evidence about phone usage obtained directly from the phone itself); *United States v. Kahler*, 236 F.Supp.3d 1009, 1021 (E.D. Mich. Feb. 14, 2017) (finding "[i]f a user who has taken special precautions to hide his IP address does not suffer a Fourth Amendment violation when a law enforcement officer compels his computer to disclose his IP address . . . and other identifying information, then it is difficult to imagine any kind of online activity which is protected by the Fourth Amendment.").

All of the above reasons are precisely why the FBI has previously sought a domestic warrant before it deployed an NIT. *See, e.g., Michaud*, 2016 WL 337263, at *1–2; *United States v. Tippens*, 773 F. App'x 383, 385 (9th Cir.), *cert. denied*, 140 S. Ct. 419, (2019). Here, there was no warrant, and as a result, all illegal fruits must be suppressed.

III. MR. SANDERS IS ENTITLED TO A *FRANKS* HEARING BECAUSE THE FBI MISLED THE MAGISTRATE IN PARAGRAPH 25 OF THE AFFIDAVIT.

In Paragraph 25, the Special Agent misrepresented both the nature of the joint venture between the US and the [redacted] and the process the [redacted] used to identify the Sanders family's IP address (along with many other IP addresses). The Special Agent suggested there was no Fourth Amendment issue because the [redacted] investigation of [redacted] was independent, and because the [redacted] did not interfere with, access, search, and/or seize data from any computers in the US. To the contrary, as Agent Ford knew or should have known, the FBI and the [redacted] were investigating the same website, at the same time, and the [redacted] actually used [redacted], pursuant to two [redacted] warrants, *see* FLA Letter (Dkt. 253-3); *see also* [redacted] Decl. 1 (Dkt. 254-7) at 2, to search and seize data from US computers, which either violated US law or required the FBI to obtain a prior warrant. *See, e.g.*, 18 U.S.C. § 1030 (prohibiting the intentional accessing of and obtaining information from a computer without authorization); 18 U.S.C. § 2511 (prohibiting the intentional interception of, any wire, oral, or electronic communication without authorization); *see also Darby*, 190 F. Supp. 3d at 530.

If Agent Ford is the Tor expert he purported himself to be in the Aff. (Dkt. 254-3), he knew or should have known that he was misleading the Magistrate about how Tor worked, the nature of the target website given that it was an onion service, and how the Internet user could

have been identified. If Agent Ford was not the Tor expert he represented himself as, he misled the Magistrate about the reliability and accuracy of his statements on those same topics.

If Paragraph 25 accurately explained to the Magistrate that the investigation between the US and the [redacted] was a joint venture and, contrary to the [redacted] assertion that it had not interfered with computers in the US, it had in fact used "[redacted]" against computers in the US to search and seize their IP addresses, that would have directly undermined the credibility of the [redacted] The entire Affidavit depended on the [redacted] credibility, *see, e.g.,* Aff. (Dkt. 254-3) at ¶ 26-27, because the FBI had no incriminating information about the Internet user apart from paragraph 23, *id.* at ¶ 23. If Paragraph 25 accurately reflected the state of Agent Ford's knowledge, it would not have obscured the true nature of the joint operation or the joint [redacted] US effort to circumvent the requirements of the Fourth Amendment. *See, e.g., Riley*, 573 U.S. at 403 (the Fourth Amendment was meant to protect against "the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity").

IV. IN THE ALTERNATIVE, IF THE [redacted] USED TRAFFIC ANALYSIS, THERE WAS NO PROBABLE CAUSE.

If the [redacted] used passive traffic analysis, as opposed to an NIT, an identification based on a single visit to a website is not sufficiently reliable or accurate to justify the search of someone's home. *See, e.g.,* Clayton Decl. (Dkt. 256-8) at ¶ 59 ("law enforcement will need to assume that every result they get from a traffic confirmation attack is potentially a false positive and . . . they will have to look for multiple identifications . . . before acting upon the data"); Murdoch Decl. (Dkt. 464-2) at ¶¶ 24-26; *id.* at ¶ 32 ("a single identification using traffic analysis could very well be a false-positive error"). Here, the FBI produced no information establishing the reliability of the method the [redacted] used to identify the Internet user's IP address. *See Harris*, 568 U.S. at 248.

Because the FBI has never alleged that the Internet user visited the target website more than once, a single visit using passive traffic analysis was likely a false identification and the identification was insufficiently reliable.

CONCLUSION

Because this was a joint venture between the FBI and the [redacted] the warrantless intrusion into Mr. Sanders's computer was illegal and the exclusionary rule applies to conduct by the [redacted] In the alternative, if the [redacted] did not intrude into Mr. Sanders's computer, it used a method that was not sufficiently reliable for the purposes of finding probable cause. In the Affidavit, Special Agent Ford deliberately misstated to the Magistrate that this was not a joint venture and that the method used was legal, accurate, and reliable. Because the warrant issued in this case was based on materially false statements and omissions with respect to Paragraph 25 of the Affidavit, the good faith exception under *Leon*, 468 U.S. at 932 does not apply. As a result, all evidence derived from the illegal search of the Sanders's family home, the illegal interrogation of Mr. Sanders and his parents, and the illegal forensic examinations of any tangible evidence should be suppressed as fruit of the poisonous tree.

Respectfully submitted,

/s/
Jonathan Jeffress (#42884)
Jade Chong-Smith (admitted *pro hac vice*)
KaiserDillon PLLC
1099 Fourteenth St., N.W.; 8th Floor—West
Washington, D.C. 20005
Telephone: (202) 683-6150
Facsimile: (202) 280-1034
Email: jjeffress@kaiserdillon.com
Email: jchong-smith@kaiserdillon.com

/s/
Nina J. Ginsberg (#19472)
Zachary Deubler (#90669)
DiMuroGinsberg, P.C.
1101 King Street, Suite 610
Alexandria, VA 22314
Telephone: (703) 684-4333
Facsimile: (703) 548-3181
Email: nginsberg@dimuro.com
Email: zdeubler@dimuro.com

/s/
Mark J. Mahoney (admitted *pro hac vice*)
Harrington & Mahoney
70 Niagara Street, 3rd Floor
Buffalo, New York 14202-3407
Telephone: 716-853-3700
Facsimile: 716-853-3710
Email: mjm@harringtonmahoney.com

/s/
H. Louis Sirkin (*pro hac vice* pending)
600 Vine Street, Suite 2700
Cincinnati, OH 45202
Telephone: (513) 721-4450
Facsimile: (513) 721-0109
Email: hls@santenhughes.com

Counsel for Defendant Zackary Ellis Sanders

CERTIFICATE OF SERVICE

I hereby certify that on this 24th day of September 2021, the foregoing was served electronically on the counsel of record through the US District Court for the Eastern District of Virginia Electronic Document Filing System (ECF) and the document is available on the ECF system.

/s/ Jonathan Jeffress
Jonathan Jeffress